(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Gebrauchsmusterschrift**

(10) **DE 298 24 256 U 1**

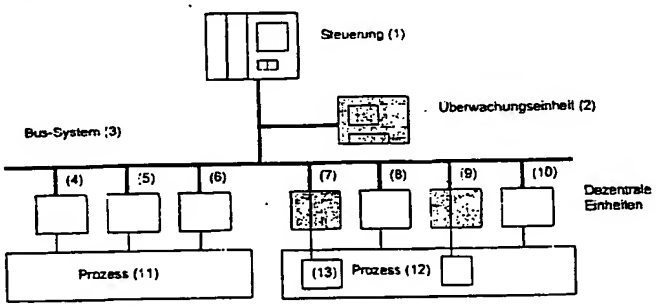
(51) Int. Cl.[7]:
G 05 B 9/02
G 05 B 19/048

(21) Aktenzeichen: 298 24 256.7
(67) Anmeldetag: 14. 12. 1998
aus Patentanmeldung: 198 57 683.8
(47) Eintragungstag: 13. 6. 2001
(43) Bekanntmachung im Patentblatt: 19. 7. 2001

(73) Inhaber:
Wratil, Peter, Dr., 21224 Rosengarten, DE

(54) Einheit zur Sicherheitsüberwachung von Steuerungseinrichtungen

(57) Einheit zur Sicherheitsüberwachung von Steuerungseinrichtungen, bei denen Speicherprogrammierbare Steuerungen oder Mikrorechner über ein Bus-System dezentrale Einheiten ansprechen, die einen Prozess sowohl im sicherheitsrelevanten als auch im nichtsicherheitsrelevanten Bereich regeln, steuern oder überwachen dadurch gekennzeichnet, dass zur Realisierung der Sicherheitsanforderung die Überwachungseinheit (2) hinzugefügt wird, die entweder ausschließlich oder vorwiegend die sicherheitsbehafteten Funktionen des Prozesses (12) mit der notwendigen Logik zur Überwachung gefahrbringender Abläufe oder Bewegungen (13) hinzugefügt wird, die selbst nur über das Bus-System (3), welches als Standard erhalten bleibt und keinerlei Zusatzfunktion bedarf, eine Hörer-Funktion erhält und damit zusätzlich zum Gesamtprozess adaptierbar ist, diese mit sicherheitsgerichteten dezentralen Einheiten (7, 9) kommuniziert und parallel zum Gesamtprozess alle Sicherheitsfunktionen überwacht und nur im Fehlerfall über die dezentralen Einheiten (7, 9) oder sonstigen Sicherheitseinrichtungen den sicheren Maschinen- bzw. Anlagenzustand herbeiführt.



DE 298 24 256 U 1

Beschreibung (298 24 256.7)

Es wird eine Einheit beschrieben, die über ein sicherheitsgerichtetes Bussystem mit dezentralen Komponenten kommuniziert und dabei sowohl den sicheren Datenverkehr als auch die Sicherheitsfunktionen überwacht.

Die hier vorgeschlagene Einheit ist in der Lage, die Steuerungseinrichtung und die Sicherheitsfunktion vollkommen zu trennen. Mit der Einheit wird es möglich, den Steuerungsteil vollständig vorher aufzubauen, zu testen und in Betrieb zu nehmen. Die sicherheitsrelevanten Komponenten lassen sich dann nachträglich hinzufügen, ohne die Steuerungsfunktion zu ändern. Auch nach der Installation beider Systeme (Steuerungseinrichtung und Sicherheitssystem) lassen sich Steuerungsfunktionen ändern, hinzufügen oder heraustrennen, ohne dass die Sicherheitsfunktion davon betroffen ist. Insbesondere besteht die Möglichkeit, alle Sicherheitsverknüpfungen im einzelnen unabhängig zu prüfen.

Diese Aufgabe wird erfindungsgemäß durch die kennzeichnenden Merkmale des Anspruchs 1 gelöst, während die weiteren Ansprüche (2-10) vorteilhafte Ausprägungen der beschriebenen Einheit darstellen.

In Fig. 1 ist die Funktionsweise der zu Grunde liegenden Einheit dargestellt. Hierbei besteht das Automatisierungssystem aus einer Steuerung, einem Bus-System und mehreren dezentralen Komponenten, die den Prozess steuern oder überwachen. Damit stellt die Fig. 1 eine typische Einrichtung dar, die (ohne die grau hinterlegten Komponenten) für alle nichtsicherheitsrelevanten Systeme geeignet sind. Die Anordnung entspricht dem heutigen Stand der Technik.

Im Detail steuert oder regelt die Steuerung (1) den gewünschten Prozess. Über das angeschlossene Bus-System (3) holt sie Daten vom Prozess (11,12) oder gibt sie Daten zum Prozess aus. Die dezentralen Einheiten (4-10) empfangen alle Daten vom Bus-System (3) oder stellen dem Prozess (11,12) ihre Daten zur Verfügung. Damit sind die dezentralen Einheiten nur vorgelagerte Ein-/Ausgabe-Baugruppen, die ohne ein Bus-System als Peripheriebaugruppen in der Speicherprogrammierbaren Steuerung zu finden sind.
Die Steuerung (1) enthält ein Programm (Software) das alle nichtsicherheitsrelevanten Vorgänge steuert oder regelt. Ferner enthält sie bereits in ihrem Programm auch die logischen Funktionen für die Sicherheitsverknüpfungen, die für sicherheitsrelevante Vorgänge notwendig sind. So enthält beispielsweise der Prozess (11) keine aber der Prozess (12) sicherheitsrelevante Vorgänge bei denen Bewegungen erfolgen, die eine Gefahr für Mensch oder Maschine darstellen (13). Obwohl die Steuerung (1) die notwendige Logik für die Sicherheitsanforderung enthält, kann sie im Fehlerfall nicht einwandfrei reagieren, da entweder sie selbst oder eine ihrer dezentralen Einheiten fehlerbehaftet sein kann, diese aber nicht kontrolliert werden. Das Steuerungssystem ist damit nicht in der Lage, einen Fehler abzuwehren, da jegliche Fehlererkennung fehlt.

Entsprechend der Aufgabe der Anmeldung nach Anspruch 1 werden zur Erreichung der sicheren Fehlererkennung und zur Prozessabschaltung die grau hinterlegten Komponenten hinzugefügt.
Die Überwachungseinheit (2) wird in der Funktion eines Hörers (Listener) an den Bus angeschlossen. Sie braucht damit nicht von der Steuerung berücksichtigt zu werden,

da sie nur passiv sich der Daten des Bus-Systems (3) bedient. Die Überwachungseinheit (2) ist über - die auf dem Bus laufenden Daten - über alle Zustände und Abläufe im Prozess und insbesondere über die Zustände der Prozessgrößen informiert.
Im Prinzip ist sie damit in der Lage, die sicherheitsrelevanten Zustände zu überprüfen. Zur Bewältigung dieser Aufgabe enthält sie ein einfaches Programm das nur die Sicherheitsfunktionen als Logik überwacht (z.B.: Gitterkontrolle, Anlaufüberwachung, Endschaltertest, usw.). Im Fehlerfall der Steuerung (1) kann damit die Überwachungseinheit (2) geeignete Maßnahmen ergreifen.
Diese Fehlererkennung funktioniert jedoch nur dann, wenn die Steuerungseinheit (1) als Verursacher fungiert. Fehler in den dezentralen Einheiten oder im Prozess werden von beiden Einheiten (Steuerungseinheit (1) oder Überwachungseinheit (2)) nicht registriert.
Eine vollständige Kontrolle gelingt daher nur mittels spezieller dezentraler Einheiten, die ihre eigene Funktion oder sogar die Sensorik im redundant Prozess abfragen. Entsprechend des Anspruchs 1 gehören zur optimalen Funktion dieser Einheit auch dezentrale Einheiten, die selbst Sicherheitsanforderungen genügen. Hierzu gehört insbesondere die Überwachung der eigenen Funktion und die Sicherheitsabschaltung im Fehlerfall (bei Ausfall des Bus-Systems (3) oder bei fehlerhaften Ein- oder Ausgabe).

Die Überwachungseinheit (2) erkennt somit eindeutig einen Fehler, sofern er im sicherheitsrelevanten Programm als Logik hinterlegt ist. Es bleibt der speziellen Projektierung überlassen, in welcher Form eine geeignete Sicherheitsabschaltung erfolgt. Im einfachsten Fall kann die Überwachungseinheit (2) das Bus-System (3) unterbrechen oder kurzschließen. Damit unterbindet sie die Datenübertragung und die dezentralen Einheiten (7, 9) fallen in einen sicheren Zustand. Denkbar ist aber auch ein gezieltes Abschalten der Stromversorgung, der entsprechenden Ausgabeeinheit oder ein langsames Herunterfahren des Prozessablaufs.

Schutzansprüche (298 24 256.7)

1. Einheit zur Sicherheitsüberwachung von Steuerungseinrichtungen, bei denen Speicherprogrammierbare Steuerungen oder Mikrorechner über ein Bus-System dezentrale Einheiten ansprechen, die einen Prozess sowohl im sicherheitsrelevanten als auch im nichtsicherheitsrelevanten Bereich regeln, steuern oder überwachen **dadurch gekennzeichnet**, dass zur Realisierung der Sicherheitsanforderung die Überwachungseinheit (2) hinzugefügt wird, die entweder ausschließlich oder vorwiegend die sicherheitsbehafteten Funktionen des Prozesses (12) mit der notwendigen Logik zur Überwachung gefahrbringender Abläufe oder Bewegungen (13) hinzugefügt wird, die selbst nur über das Bus-System (3), welches als Standard erhalten bleibt und keinerlei Zusatzfunktion bedarf, eine Hörer-Funktion erhält und damit zusätzlich zum Gesamtprozess adaptierbar ist, diese mit sicherheitsgerichteten dezentralen Einheiten (7,9) kommuniziert und parallel zum Gesamtprozess alle Sicherheitsfunktionen überwacht und nur im Fehlerfall über die dezentralen Einheiten (7,9) oder sonstigen Sicherheitseinrichtungen den sicheren Maschinen- bzw. Anlagenzustand herbeiführt.
2. Einheit nach Anspruch 1, dadurch gekennzeichnet, dass die Überwachungseinheit (2) über eine in der Programmiersprache festgelegten Logik verfügt, die entweder ausschließlich oder vorwiegend Sicherheitsvorgänge überwacht und damit redundant zur Gesamtsteuerung arbeitet.
3. Einheit nach den Ansprüchen 1 und 2, dadurch gekennzeichnet, dass die Überwachungseinheit (2) auch nach der Funktionskontrolle des nicht redundanten Steuerungssystems mit ihren für die Sicherheit notwendigen Abschaltfunktionen adaptierbar ist und durch ihre Sicherheitsfunktion der geforderte Grad an Sicherheit projektiert werden kann.
4. Einheit nach den Ansprüchen 1 bis 3, dadurch gekennzeichnet, dass die Überwachungseinheit (2) und die sicherheitsgerichteten dezentralen Einheiten (7,9) deaktiviert werden können, ohne die einkanalige Steuerungsfunktion zu beeinträchtigen.
5. Einheit nach den Ansprüchen 1 bis 4, dadurch gekennzeichnet, dass durch eine bustechnische Mithörfunktion der Überwachungseinheit (2) keine Rückwirkung auf den eigentlichen Steuerungsprozess entsteht, so dass eine weitgehende Trennung zwischen der Hard- und Software des nicht redundanten Steuerungssystems und der Sicherheitsüberwachung ermöglicht wird.
6. Einheit nach den Ansprüchen 1 bis 5, dadurch gekennzeichnet, dass die Überwachungseinheit (2) über den normalen Datenverkehr des Bus-Systems (3) der Steuerungseinheit (1) alle notwendigen Zustände und Funktionen erhält, die zur Überwachung des nicht redundanten Steuerungssystems notwendig sind.
7. Einheit nach den Ansprüchen 1 bis 6, dadurch gekennzeichnet, dass es an Standardbussysteme ohne Sicherheitsprotokollerweiterung adaptierbar bzw. einbindbar ist.
8. Einheit nach den Ansprüchen 1 bis 7, dadurch gekennzeichnet, dass die dezentralen Einheiten, die sicherheitsrelevante Funktionen erfassen und ansteuern, selbst ihre Funktion überwachen, möglicherweise Sensoren oder Aktoren redundant überwachen und bei Ausfall einer Funktion, beispielsweise bei Ausfall der Bus-Funktion, in den sichern Zustand schalten, der keine Gefahr mehr für Mensch oder Maschine darstellt.
9. Einheit nach den Ansprüchen 1 bis 8, dadurch gekennzeichnet, dass die Überwachungseinheit (2) in einer von dem nicht redundanten Steuerungssystem

unabhängigen Programmier- und Parametriersprache in ihren Sicherheitsfunktionen generiert werden.

10. Einheit nach den Ansprüchen 1 bis 9, dadurch gekennzeichnet, dass die Überwachungseinheit (2) neben der Überwachungsfunktion auch die Bedienung und Programmierung mittels eines integrierten Mensch-Maschinen-Interfaces erlaubt.

Zeichnung (298 24 256.7)

Fig. 1